Gestionar cuentas

Element Software

NetApp
November 12, 2025

Tabla de contenidos

Gestionar cuentas . . . 1
- Gestionar cuentas . . . 1
  - Para más información . . . 1
- Trabajar con cuentas que utilizan CHAP . . . 1
  - algoritmos CHAP . . . 1
  - Crea una cuenta . . . 2
  - Ver detalles de la cuenta . . . 2
  - Editar una cuenta . . . 3
  - Eliminar una cuenta . . . 3
  - Encuentra más información . . . 4
- Administrar cuentas de usuario de administrador de clúster . . . 4
  - tipos de cuentas de administrador de clúster de almacenamiento . . . 4
  - Ver detalles de administración del clúster . . . 4
  - Crea una cuenta de administrador de clúster . . . 5
  - Editar permisos de administrador del clúster . . . 6
  - Cambiar las contraseñas de las cuentas de administrador del clúster . . . 7
- Administrar LDAP . . . 7
  - Complete los pasos de preconfiguración para la compatibilidad con LDAP. . . . 8
  - Habilite la autenticación LDAP con la interfaz de usuario de Element. . . . 8
  - Habilite la autenticación LDAP con la API de Element. . . . 10
  - Ver detalles de LDAP . . . 13
  - Prueba la configuración LDAP . . . 13
  - Deshabilitar LDAP . . . 15
  - Encuentra más información . . . 15

Gestionar cuentas

Gestionar cuentas

En los sistemas de almacenamiento SolidFire , los inquilinos pueden usar cuentas para permitir que los clientes se conecten a volúmenes en un clúster. Cuando se crea un volumen, este se asigna a una cuenta específica. También puede administrar las cuentas de administrador de clúster para un sistema de almacenamiento SolidFire .

- "Trabajar con cuentas que utilizan CHAP"
- "Administrar cuentas de usuario de administrador de clúster"

Para más información

- "Documentación del software SolidFire y Element"
- "Plugin de NetApp Element para vCenter Server"

Trabajar con cuentas que utilizan CHAP

En los sistemas de almacenamiento SolidFire , los inquilinos pueden usar cuentas para permitir que los clientes se conecten a volúmenes en un clúster. Una cuenta contiene el protocolo de autenticación Challenge-Handshake Authentication Protocol (CHAP) necesario para acceder a los volúmenes que le han sido asignados. Cuando se crea un volumen, este se asigna a una cuenta específica.

Una cuenta puede tener asignados hasta dos mil volúmenes, pero un volumen solo puede pertenecer a una cuenta.

algoritmos CHAP

A partir del Elemento 12.7, se admiten los algoritmos CHAP seguros compatibles con FIPS SHA1, SHA-256 y SHA3-256. Cuando un iniciador iSCSI de host crea una sesión iSCSI con un destino iSCSI de Element, solicita una lista de algoritmos CHAP para usar. El destino iSCSI de Element elige el primer algoritmo que admite de la lista solicitada por el iniciador iSCSI del host. Para confirmar que el destino iSCSI de Element elige el algoritmo más seguro, debe configurar el iniciador iSCSI del host para que envíe una lista de algoritmos ordenados desde el más seguro, por ejemplo, SHA3-256, hasta el menos seguro, por ejemplo, SHA1 o MD5. Cuando el iniciador iSCSI del host no solicita algoritmos SHA, el destino iSCSI de Element elige MD5, suponiendo que la lista de algoritmos propuestos por el host contiene MD5. Es posible que deba actualizar la configuración del iniciador iSCSI del host para habilitar la compatibilidad con los algoritmos de seguridad.

Durante una actualización a Element 12.7 o posterior, si ya ha actualizado la configuración del iniciador iSCSI del host para enviar una solicitud de sesión con una lista que incluye algoritmos SHA, a medida que se reinician los nodos de almacenamiento, se activan los nuevos algoritmos seguros y se establecen sesiones iSCSI nuevas o reconectadas utilizando el protocolo más seguro. Todas las sesiones iSCSI existentes pasarán de MD5 a SHA durante la actualización. Si no actualiza la configuración del iniciador iSCSI del host para solicitar SHA, las sesiones iSCSI existentes seguirán utilizando MD5. Posteriormente, después de actualizar los algoritmos CHAP del iniciador iSCSI del host, las sesiones iSCSI deberían pasar gradualmente de MD5 a SHA con el tiempo, en función de las actividades de mantenimiento que resulten en reconexiones

de sesiones iSCSI.

Por ejemplo, el iniciador iSCSI de host predeterminado en Red Hat Enterprise Linux (RHEL) 8.3 tiene el `node.session.auth.chap_algs = SHA3-256,SHA256,SHA1,MD5` Se ha comentado la configuración, lo que provoca que el iniciador iSCSI solo utilice MD5. Descomentar esta configuración en el host y reiniciar el iniciador iSCSI activa las sesiones iSCSI desde ese host para que comiencen a usar SHA3-256.

Si es necesario, puede utilizar el "Lista de sesiones ISCSIS" Método API para ver los algoritmos CHAP que se utilizan en cada sesión.

Crea una cuenta

Es posible crear una cuenta para permitir el acceso a los volúmenes.

Cada nombre de cuenta en el sistema debe ser único.

1. Seleccione **Administración** > **Cuentas**.
2. Haz clic en **Crear cuenta**.
3. Introduce un **Nombre de usuario**.
4. En la sección **Configuración CHAP**, introduzca la siguiente información:

   Deje los campos de credenciales en blanco para generar automáticamente cualquiera de las contraseñas.

   - **Secreto del iniciador** para la autenticación de sesión de nodo CHAP.
   - **Secreto de destino** para la autenticación de sesión de nodo CHAP.
5. Haz clic en **Crear cuenta**.

Ver detalles de la cuenta

Puede visualizar la actividad de rendimiento de cuentas individuales en formato gráfico.

La información del gráfico proporciona información sobre las operaciones de entrada/salida y el rendimiento de la cuenta. Los niveles de actividad promedio y máximo se muestran en incrementos de períodos de reporte de 10 segundos. Estas estadísticas incluyen la actividad de todos los volúmenes asignados a la cuenta.

1. Seleccione **Administración** > **Cuentas**.
2. Haz clic en el icono de Acciones para una cuenta.
3. Haga clic en **Ver detalles**.

Aquí tenéis algunos detalles:

- **Estado**: El estado de la cuenta. Valores posibles:
  - activa: Una cuenta activa.
  - bloqueado: Una cuenta bloqueada.
  - Eliminada: Una cuenta que ha sido borrada y purgada.
- **Volúmenes activos**: El número de volúmenes activos asignados a la cuenta.
- **Compresión**: La puntuación de eficiencia de compresión para los volúmenes asignados a la cuenta.

- **Desduplicación**: La puntuación de eficiencia de deduplicación para los volúmenes asignados a la cuenta.
- **Aprovisionamiento ligero**: La puntuación de eficiencia del aprovisionamiento ligero para los volúmenes asignados a la cuenta.
- **Eficiencia general**: La puntuación de eficiencia general para los volúmenes asignados a la cuenta.

Editar una cuenta

Puedes editar una cuenta para cambiar el estado, cambiar las claves CHAP o modificar el nombre de la cuenta.

Modificar la configuración CHAP en una cuenta o eliminar iniciadores o volúmenes de un grupo de acceso puede provocar que los iniciadores pierdan el acceso a los volúmenes de forma inesperada. Para verificar que el acceso al volumen no se pierda inesperadamente, cierre siempre las sesiones iSCSI que se verán afectadas por un cambio de cuenta o de grupo de acceso, y verifique que los iniciadores puedan volver a conectarse a los volúmenes después de que se hayan completado los cambios en la configuración del iniciador y la configuración del clúster.

Los volúmenes persistentes asociados a los servicios de administración se asignan a una nueva cuenta que se crea durante la instalación o actualización. Si utiliza volúmenes persistentes, no modifique ni elimine la cuenta asociada.

1. Seleccione **Administración** > **Cuentas**.
2. Haz clic en el icono de Acciones para una cuenta.
3. En el menú que aparece, seleccione **Editar**.
4. **Opcional:** Edita el **Nombre de usuario**.
5. **Opcional:** Haga clic en la lista desplegable **Estado** y seleccione un estado diferente.

   Al cambiar el estado a **bloqueado**, se terminan todas las conexiones iSCSI a la cuenta y esta deja de ser accesible. Los volúmenes asociados a la cuenta se mantienen; sin embargo, no son detectables mediante iSCSI.

6. **Opcional:** En **Configuración CHAP**, edite las credenciales **Secreto del iniciador** y **Secreto del destino** utilizadas para la autenticación de la sesión del nodo.

   Si no modifica las credenciales de **Configuración CHAP**, estas permanecerán sin cambios. Si dejas en blanco los campos de credenciales, el sistema generará nuevas contraseñas.

7. Haz clic en **Guardar cambios**.

Eliminar una cuenta

Puedes eliminar una cuenta cuando ya no sea necesaria.

Elimine y purgue cualquier volumen asociado con la cuenta antes de eliminar la cuenta.

Los volúmenes persistentes asociados a los servicios de administración se asignan a una nueva cuenta que se crea durante la instalación o actualización. Si utiliza volúmenes persistentes, no modifique ni elimine la cuenta asociada.

1. Seleccione **Administración** > **Cuentas**.
2. Haz clic en el icono de Acciones de la cuenta que deseas eliminar.
3. En el menú que aparece, seleccione **Eliminar**.
4. Confirma la acción.

Encuentra más información

- "Documentación del software SolidFire y Element"
- "Plugin de NetApp Element para vCenter Server"

Administrar cuentas de usuario de administrador de clúster

Puede administrar las cuentas de administrador de clúster para un sistema de almacenamiento SolidFire creando, eliminando y editando cuentas de administrador de clúster, cambiando la contraseña de administrador de clúster y configurando los ajustes de LDAP para administrar el acceso al sistema para los usuarios.

tipos de cuentas de administrador de clúster de almacenamiento

En un clúster de almacenamiento que ejecuta el software NetApp Element , pueden existir dos tipos de cuentas de administrador: la cuenta de administrador principal del clúster y una cuenta de administrador del clúster.

- **Cuenta de administrador principal del clúster**

  Esta cuenta de administrador se crea cuando se crea el clúster. Esta cuenta es la cuenta administrativa principal con el nivel más alto de acceso al clúster. Esta cuenta es análoga a un usuario root en un sistema Linux. Puedes cambiar la contraseña de esta cuenta de administrador.

- **Cuenta de administrador del clúster**

  Puede otorgar a una cuenta de administrador de clúster un rango limitado de acceso administrativo para realizar tareas específicas dentro de un clúster. Las credenciales asignadas a cada cuenta de administrador del clúster se utilizan para autenticar las solicitudes de API y de la interfaz de usuario de Element dentro del sistema de almacenamiento.

> Se requiere una cuenta de administrador de clúster local (no LDAP) para acceder a los nodos activos de un clúster a través de la interfaz de usuario por nodo. No se requieren credenciales de cuenta para acceder a un nodo que aún no forma parte de un clúster.

Ver detalles de administración del clúster

1. Para crear una cuenta de administrador de clúster (no LDAP) para todo el clúster, realice las siguientes acciones:
   a. Haz clic en **Usuarios** > **Administradores del clúster**.
2. En la página Administradores del clúster de la pestaña Usuarios, puede ver la siguiente información.
   - **ID**: Número secuencial asignado a la cuenta del administrador del clúster.

- **Nombre de usuario**: El nombre asignado a la cuenta de administrador del clúster cuando se creó.
- **Acceso**: Los permisos de usuario asignados a la cuenta de usuario. Valores posibles:
  - leer
  - informes
  - nodos
  - unidades
  - volúmenes
  - cuentas
  - administradores de clúster
  - administrador
  - Administrador de soporte

> Todos los permisos están disponibles para el tipo de acceso de administrador.
>
> Existen tipos de acceso disponibles a través de la API que no están disponibles en la interfaz de usuario de Element.

+

- **Tipo**: El tipo de administrador del clúster. Valores posibles:
  - Grupo
  - LDAP
- **Atributos**: Si la cuenta de administrador del clúster se creó utilizando la API de Element, esta columna muestra cualquier par nombre-valor que se haya establecido utilizando ese método.

  Ver"Referencia de la API de NetApp Element Software" .

Crea una cuenta de administrador de clúster

Puede crear nuevas cuentas de administrador de clúster con permisos para permitir o restringir el acceso a áreas específicas del sistema de almacenamiento. Cuando configuras los permisos de la cuenta de administrador del clúster, el sistema otorga derechos de solo lectura para cualquier permiso que no asignes al administrador del clúster.

Si desea crear una cuenta de administrador de clúster LDAP, asegúrese de que LDAP esté configurado en el clúster antes de comenzar.

"Habilite la autenticación LDAP con la interfaz de usuario de Element."

Posteriormente, puede cambiar los privilegios de la cuenta de administrador del clúster para la generación de informes, nodos, unidades, volúmenes, cuentas y acceso a nivel de clúster. Cuando habilitas un permiso, el sistema asigna acceso de escritura para ese nivel. El sistema otorga al usuario administrador acceso de solo lectura para los niveles que usted no seleccione.

Posteriormente también podrá eliminar cualquier cuenta de usuario administrador del clúster creada por un administrador del sistema. No se puede eliminar la cuenta de administrador principal del clúster que se creó cuando se creó el clúster.

1. Para crear una cuenta de administrador de clúster (no LDAP) para todo el clúster, realice las siguientes acciones:
   a. Haz clic en **Usuarios** > **Administradores del clúster**.
   b. Haga clic en **Crear administrador de clúster**.
   c. Seleccione el tipo de usuario **Cluster**.
   d. Introduce un nombre de usuario y una contraseña para la cuenta y confirma la contraseña.
   e. Seleccione los permisos de usuario que se aplicarán a la cuenta.
   f. Seleccione la casilla de verificación para aceptar el Acuerdo de Licencia de Usuario Final.
   g. Haga clic en **Crear administrador de clúster**.
2. Para crear una cuenta de administrador de clúster en el directorio LDAP, realice las siguientes acciones:
   a. Haga clic en **Clúster** > **LDAP**.
   b. Asegúrese de que la autenticación LDAP esté habilitada.
   c. Haz clic en **Probar autenticación de usuario** y copia el nombre distintivo que aparece para el usuario o uno de los grupos a los que pertenece el usuario para que puedas pegarlo más tarde.
   d. Haz clic en **Usuarios** > **Administradores del clúster**.
   e. Haga clic en **Crear administrador de clúster**.
   f. Seleccione el tipo de usuario LDAP.
   g. En el campo Nombre distintivo, siga el ejemplo del cuadro de texto para introducir un nombre distintivo completo para el usuario o grupo. Como alternativa, péguelo del nombre distinguido que copió anteriormente.

      Si el nombre distinguido forma parte de un grupo, cualquier usuario que sea miembro de ese grupo en el servidor LDAP tendrá los permisos de esta cuenta de administrador.

   Para agregar usuarios o grupos de administradores de clúster LDAP, el formato general del nombre de usuario es “LDAP:<Nombre distinguido completo>”.

   a. Seleccione los permisos de usuario que se aplicarán a la cuenta.
   b. Seleccione la casilla de verificación para aceptar el Acuerdo de Licencia de Usuario Final.
   c. Haga clic en **Crear administrador de clúster**.

Editar permisos de administrador del clúster

Puede cambiar los privilegios de la cuenta de administrador del clúster para la generación de informes, nodos, unidades, volúmenes, cuentas y acceso a nivel de clúster. Cuando habilitas un permiso, el sistema asigna acceso de escritura para ese nivel. El sistema otorga al usuario administrador acceso de solo lectura para los niveles que usted no seleccione.

1. Haz clic en **Usuarios** > **Administradores del clúster**.
2. Haga clic en el icono Acciones del administrador del clúster que desea editar.
3. Haga clic en **Editar**.
4. Seleccione los permisos de usuario que se aplicarán a la cuenta.
5. Haz clic en **Guardar cambios**.

Cambiar las contraseñas de las cuentas de administrador del clúster

Puede utilizar la interfaz de usuario de Element para cambiar las contraseñas de administrador del clúster.

1. Haz clic en **Usuarios** > **Administradores del clúster**.
2. Haga clic en el icono Acciones del administrador del clúster que desea editar.
3. Haga clic en **Editar**.
4. En el campo Cambiar contraseña, introduzca una nueva contraseña y confírmela.
5. Haz clic en **Guardar cambios**.

Información relacionada

- "Obtenga información sobre los tipos de acceso disponibles para las API de Element."
- "Habilite la autenticación LDAP con la interfaz de usuario de Element."
- "Deshabilitar LDAP"
- "Plugin de NetApp Element para vCenter Server"

Administrar LDAP

Puede configurar el Protocolo Ligero de Acceso a Directorios (LDAP) para habilitar la funcionalidad de inicio de sesión segura basada en directorios para el almacenamiento SolidFire . Puede configurar LDAP a nivel de clúster y autorizar usuarios y grupos LDAP.

La gestión de LDAP implica configurar la autenticación LDAP en un clúster SolidFire utilizando un entorno de Microsoft Active Directory existente y probar la configuración.

Puedes utilizar direcciones IPv4 e IPv6.

Habilitar LDAP implica los siguientes pasos generales, descritos en detalle:

1. **Complete los pasos de preconfiguración para la compatibilidad con LDAP**. Compruebe que dispone de todos los datos necesarios para configurar la autenticación LDAP.
2. **Habilitar la autenticación LDAP**. Utilice la interfaz de usuario de Element o la API de Element.
3. **Validar la configuración LDAP**. Opcionalmente, verifique que el clúster esté configurado con los valores correctos ejecutando el método de la API GetLdapConfiguration o revisando la configuración de LCAP mediante la interfaz de usuario de Element.
4. **Prueba la autenticación LDAP** (con el `readonly` usuario). Compruebe que la configuración LDAP es correcta ejecutando el método API TestLdapAuthentication o utilizando la interfaz de usuario de Element. Para esta prueba inicial, utilice el nombre de usuario “sAMAccountName” de `readonly` usuario. Esto validará que su clúster esté configurado correctamente para la autenticación LDAP y también validará que el `readonly` Las credenciales y el acceso son correctos. Si este paso falla, repita los pasos del 1 al 3.
5. **Prueba la autenticación LDAP** (con una cuenta de usuario que quieras agregar). Repita el paso 4 con una cuenta de usuario que desee agregar como administrador del clúster de Element. Copia el `distinguished` nombre (DN) o el usuario (o el grupo). Este DN se utilizará en el paso 6.
6. **Agregue el administrador del clúster LDAP** (copie y pegue el DN del paso de prueba de autenticación LDAP). Utilizando la interfaz de usuario de Element o el método de la API AddLdapClusterAdmin, cree un nuevo usuario administrador de clúster con el nivel de acceso adecuado. Para el nombre de usuario, pegue el DN completo que copió en el paso 5. Esto garantiza que el DN esté formateado correctamente.

7. **Prueba el acceso de administrador del clúster**. Inicie sesión en el clúster utilizando el usuario administrador del clúster LDAP recién creado. Si has añadido un grupo LDAP, puedes iniciar sesión como cualquier usuario de ese grupo.

Complete los pasos de preconfiguración para la compatibilidad con LDAP.

Antes de habilitar la compatibilidad con LDAP en Element, debe configurar un servidor de Active Directory de Windows y realizar otras tareas de preconfiguración.

Pasos

1. Configurar un servidor de directorio activo de Windows.
2. **Opcional:** Habilitar la compatibilidad con LDAPS.
3. Crear usuarios y grupos.
4. Cree una cuenta de servicio de solo lectura (como “sfreadonly”) para usarla para buscar en el directorio LDAP.

Habilite la autenticación LDAP con la interfaz de usuario de Element.

Puede configurar la integración del sistema de almacenamiento con un servidor LDAP existente. Esto permite a los administradores de LDAP gestionar de forma centralizada el acceso de los usuarios al sistema de almacenamiento.

Puede configurar LDAP mediante la interfaz de usuario de Element o la API de Element. Este procedimiento describe cómo configurar LDAP utilizando la interfaz de usuario de Element.

Este ejemplo muestra cómo configurar la autenticación LDAP en SolidFire y utiliza `SearchAndBind` como tipo de autenticación. El ejemplo utiliza un único servidor Active Directory de Windows Server 2012 R2.

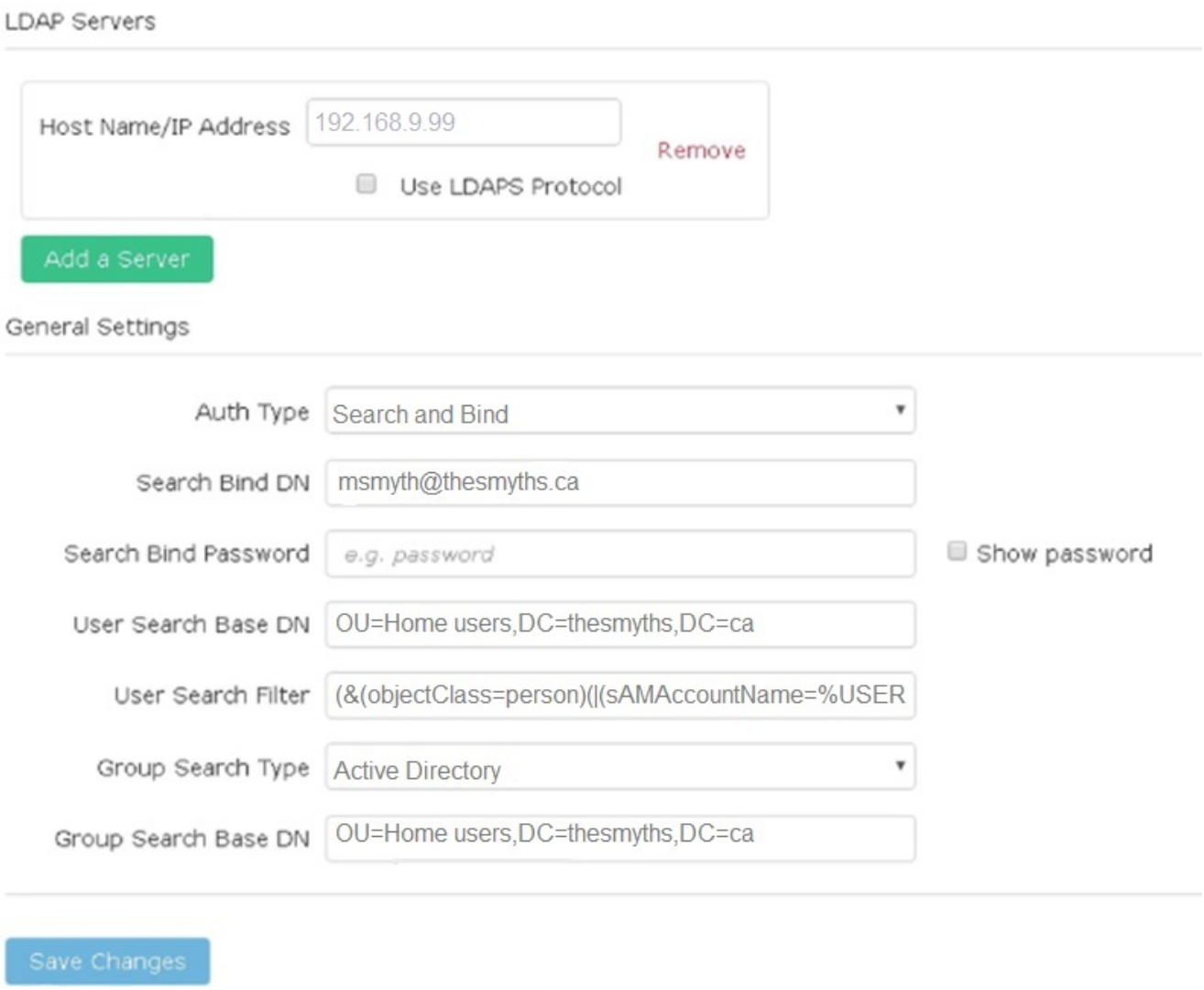
Pasos

1. Haga clic en **Clúster** > **LDAP**.
2. Haga clic en **Sí** para habilitar la autenticación LDAP.
3. Haz clic en **Añadir un servidor**.
4. Introduzca el **Nombre de host/Dirección IP**.

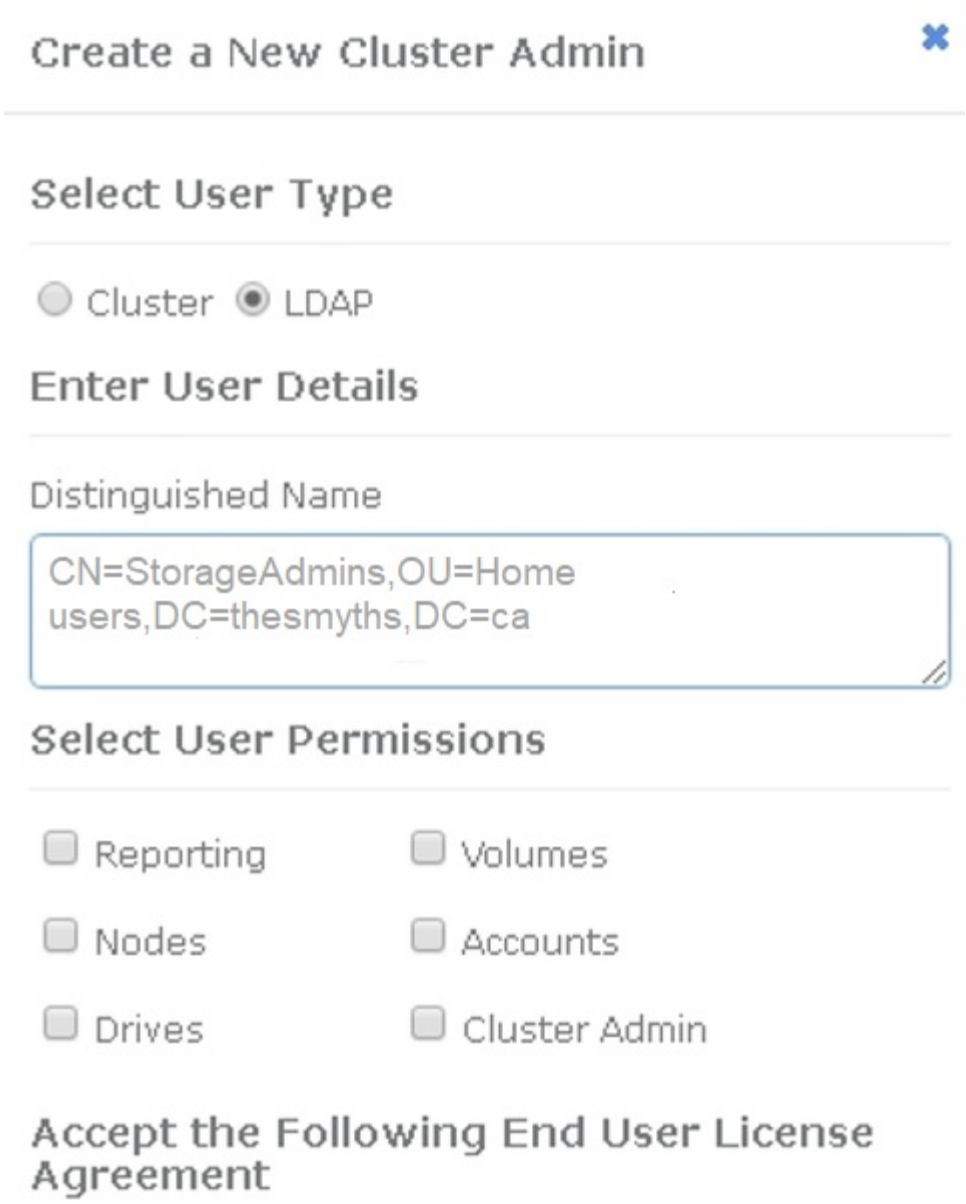
   También se puede introducir un número de puerto personalizado opcional.

   Por ejemplo, para agregar un número de puerto personalizado, ingrese <nombre de host o dirección IP>:<número de puerto>

5. **Opcional:** Seleccione **Usar protocolo LDAPS**.
6. Introduzca la información requerida en **Ajustes generales**.



7. Haga clic en **Habilitar LDAP**.
8. Haz clic en **Probar autenticación de usuario** si quieres probar el acceso al servidor de un usuario.
9. Copie el nombre distintivo y la información del grupo de usuarios que aparece para utilizarlos posteriormente al crear administradores de clúster.
10. Haz clic en **Guardar cambios** para guardar la nueva configuración.
11. Para crear un usuario en este grupo para que cualquiera pueda iniciar sesión, complete lo siguiente:
    a. Haz clic en **Usuario** > **Ver**.



b. Para el nuevo usuario, haga clic en **LDAP** para Tipo de usuario y pegue el grupo que copió en el campo Nombre distintivo.
c. Seleccione los permisos, normalmente todos los permisos.
d. Desplácese hacia abajo hasta el Acuerdo de Licencia de Usuario Final y haga clic en **Acepto**.
e. Haga clic en **Crear administrador de clúster**.

   Ahora tienes un usuario con el valor de un grupo de Active Directory.

Para probar esto, cierre sesión en la interfaz de usuario de Element y vuelva a iniciar sesión como usuario de ese grupo.

Habilite la autenticación LDAP con la API de Element.

Puede configurar la integración del sistema de almacenamiento con un servidor LDAP existente. Esto permite a los administradores de LDAP gestionar de forma centralizada el acceso de los usuarios al sistema de almacenamiento.

Puede configurar LDAP mediante la interfaz de usuario de Element o la API de Element. Este procedimiento describe cómo configurar LDAP utilizando la API de Element.

Para aprovechar la autenticación LDAP en un clúster de SolidFire , primero debe habilitar la autenticación LDAP en el clúster mediante el siguiente método: `EnableLdapAuthentication` Método API.

Pasos

1. Habilite primero la autenticación LDAP en el clúster utilizando `EnableLdapAuthentication` Método API.
2. Ingrese la información requerida.

```
{
     "method":"EnableLdapAuthentication",
     "params":{
          "authType": "SearchAndBind",
          "groupSearchBaseDN": "dc=prodtest,dc=solidfire,dc=net",
          "groupSearchType": "ActiveDirectory",
          "searchBindDN": "SFReadOnly@prodtest.solidfire.net",
          "searchBindPassword": "ReadOnlyPW",
          "userSearchBaseDN": "dc=prodtest,dc=solidfire,dc=net ",
          "userSearchFilter":
"(&(objectClass=person)(sAMAccountName=%USERNAME%))"
          "serverURIs": [
               "ldap://172.27.1.189",
          [
     },
  "id":"1"
}
```

3. Cambie los valores de los siguientes parámetros:

Parámetros utilizados	Descripción
Tipo de autenticación: Buscar y vincular	Indica que el clúster utilizará la cuenta de servicio de solo lectura para buscar primero al usuario que se está autenticando y, posteriormente, vincularlo si se encuentra y se autentica.
groupSearchBaseDN: dc=prodtest,dc=solidfire,dc=net	Especifica la ubicación en el árbol LDAP donde comenzar la búsqueda de grupos. Para este ejemplo, hemos utilizado la raíz de nuestro árbol. Si su árbol LDAP es muy grande, es posible que desee configurarlo en un subárbol más granular para disminuir los tiempos de búsqueda.

Parámetros utilizados	Descripción
userSearchBaseDN: dc=prodtest,dc=solidfire,dc=net	Especifica la ubicación en el árbol LDAP donde comenzar la búsqueda de usuarios. Para este ejemplo, hemos utilizado la raíz de nuestro árbol. Si su árbol LDAP es muy grande, es posible que desee configurarlo en un subárbol más granular para disminuir los tiempos de búsqueda.
groupSearchType: ActiveDirectory	Utiliza el servidor Active Directory de Windows como servidor LDAP.

`userSearchFilter: "(&(objectClass=person)(sAMAccountName=%USERNAME%))"`
 	
Para usar el nombre principal de usuario (dirección de correo electrónico para iniciar sesión), puede cambiar el filtro de búsqueda de usuario a:
 	
`"(&(objectClass=person)(userPrincipalName=%USERNAME%))"`
 	
O bien, para buscar tanto userPrincipalName como sAMAccountName, puede utilizar el siguiente userSearchFilter:
 	
`"(&(objectClass=person)(`
	(sAMAccountName=%USERNAME%)(userPrincipalName=%USERNAME%)))" ----

Utilizamos sAMAccountName como nombre de usuario para iniciar sesión en el clúster SolidFire . Estos ajustes le indican a LDAP que busque el nombre de usuario especificado durante el inicio de sesión en el atributo sAMAccountName y también que limite la búsqueda a las entradas que tengan "person" como valor en el atributo objectClass.	searchBindDN
Este es el nombre distintivo del usuario de solo lectura que se utilizará para buscar en el directorio LDAP. Para Active Directory, lo más sencillo suele ser utilizar el nombre principal de usuario (formato de dirección de correo electrónico) para el usuario.	buscarContraseñaVinculada

Para probar esto, cierre sesión en la interfaz de usuario de Element y vuelva a iniciar sesión como usuario de ese grupo.

Ver detalles de LDAP

Consulte la información LDAP en la página LDAP de la pestaña Clúster.

Debe habilitar LDAP para ver esta configuración de LDAP.

1. Para ver los detalles de LDAP con la interfaz de usuario de Element, haga clic en **Clúster** > **LDAP**.
   - **Nombre de host/Dirección IP**: Dirección de un servidor de directorio LDAP o LDAPS.
   - **Tipo de autenticación**: El método de autenticación del usuario. Valores posibles:
     - Enlace directo
     - Buscar y enlazar
   - **DN de enlace de búsqueda**: Un DN completo para iniciar sesión y realizar una búsqueda LDAP del usuario (necesita acceso de nivel de enlace al directorio LDAP).
   - **Contraseña de enlace de búsqueda**: Contraseña utilizada para autenticar el acceso al servidor LDAP.
   - **DN base de búsqueda de usuarios**: El DN base del árbol utilizado para iniciar la búsqueda de usuarios. El sistema busca en el subárbol desde la ubicación especificada.
   - **Filtro de búsqueda de usuario**: Introduzca lo siguiente utilizando su nombre de dominio:

     ```
     (&(objectClass=person)(|(sAMAccountName=%USERNAME%)(userPrincipalName=%USERNAME%)))
     ```

   - **Tipo de búsqueda de grupo**: Tipo de búsqueda que controla el filtro de búsqueda de grupo predeterminado utilizado. Valores posibles:
     - Active Directory: Membresía anidada de todos los grupos LDAP de un usuario.
     - Sin grupos: No hay soporte para grupos.
     - DN de miembro: Grupos de estilo DN de miembro (de un solo nivel).
   - **DN base de búsqueda de grupo**: El DN base del árbol utilizado para iniciar la búsqueda de grupo. El sistema busca en el subárbol desde la ubicación especificada.
   - **Prueba de autenticación de usuario**: Después de configurar LDAP, utilice esto para probar la autenticación de nombre de usuario y contraseña para el servidor LDAP. Introduce una cuenta que ya exista para probar esto. Aparece el nombre distintivo y la información del grupo de usuarios, que puede copiar para su uso posterior al crear administradores de clúster.

Prueba la configuración LDAP

Tras configurar LDAP, debe probarlo utilizando la interfaz de usuario de Element o la API de Element. `TestLdapAuthentication` método.

Pasos

1. Para probar la configuración LDAP con la interfaz de usuario de Element, haga lo siguiente:
   a. Haga clic en **Clúster** > **LDAP**.
   b. Haga clic en **Probar autenticación LDAP**.
   c. Resuelva cualquier problema utilizando la información de la siguiente tabla:

Mensaje de error	Descripción
`xLDAPUserNotFound`	• No se encontró al usuario que se estaba probando en la configuración. `userSearchBaseDN` subárbol. • El `userSearchFilter` está configurado incorrectamente.
`xLDAPBindFailed (Error: Invalid credentials)`	• El nombre de usuario que se está probando es un usuario LDAP válido, pero la contraseña proporcionada es incorrecta. • El nombre de usuario que se está probando es un usuario LDAP válido, pero la cuenta está actualmente deshabilitada.
`xLDAPSearchBindFailed (Error: Can't contact LDAP server)`	La URI del servidor LDAP es incorrecta.
`xLDAPSearchBindFailed (Error: Invalid credentials)`	El nombre de usuario o la contraseña de solo lectura están configurados incorrectamente.
`xLDAPSearchFailed (Error: No such object)`	El `userSearchBaseDN` no es una ubicación válida dentro del árbol LDAP.
`xLDAPSearchFailed (Error: Referral)`	• El `userSearchBaseDN` no es una ubicación válida dentro del árbol LDAP. • El `userSearchBaseDN` y `groupSearchBaseDN` están en una unidad organizativa anidada. Esto puede causar problemas de permisos. La solución alternativa consiste en incluir la OU en las entradas DN base de usuario y grupo, (por ejemplo: `ou=storage, cn=company, cn=com`)

2. Para probar la configuración LDAP con la API de Element, haga lo siguiente:
   a. Llama al método TestLdapAuthentication.

```
{
  "method":"TestLdapAuthentication",
     "params":{
        "username":"admin1",
        "password":"admin1PASS
      },
      "id": 1
}
```

b. Revisa los resultados. Si la llamada a la API se realiza correctamente, los resultados incluyen el nombre distintivo del usuario especificado y una lista de los grupos a los que pertenece el usuario.

```
{
"id": 1
     "result": {
         "groups": [

"CN=StorageMgmt,OU=PTUsers,DC=prodtest,DC=solidfire,DC=net"
         ],
         "userDN": "CN=Admin1
Jones,OU=PTUsers,DC=prodtest,DC=solidfire,DC=net"
     }
}
```

Deshabilitar LDAP

Puede deshabilitar la integración LDAP mediante la interfaz de usuario de Element.

Antes de comenzar, debe anotar todas las opciones de configuración, ya que deshabilitar LDAP borra todas las configuraciones.

Pasos

1. Haga clic en **Clúster** > **LDAP**.
2. Haga clic en **No**.
3. Haga clic en **Deshabilitar LDAP**.

Encuentra más información

- "Documentación del software SolidFire y Element"
- "Plugin de NetApp Element para vCenter Server"